UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,972	08/20/2001	Philip Hawkes	010497	7964

23696 7590 08/03/2006

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/933,972	HAWKES ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 6/8/2006 was received and considered.

2. Claims 1-24 are pending.

Response to Arguments

3. Applicant's arguments filed 6/8/2006 have been fully considered but they are not persuasive.

4. Applicant's response (§I) overcomes the claim objection to claim (renumbered as) 13.

5. Applicant's response (§II) are not persuasive.

6. Applicant's response (p. 11) argues that Richards uses CCK_1 as a key to decrypt [CCK_1]CCK_1 (Richards, col. 15). Applicant then bases the argument that the second key to which the examiner refers (PK and SK) is not used to encrypt/decrypt the broadcast content. However, Applicant is directed to Richards, col. 14, lines 46-67. Here, Richards discloses that the invention also has the capability for video-on-demand, where a user can purchase a single program and not the package. However, this is a different embodiment (Fig. 25) than the embodiment (standard broadcast using the UEV as the rook key) used in the rejection and disclosed in Fig. 26. In this embodiment (Fig. 26), SK is used to encrypt/decrypt the content along with PK which protects SK. The content program key (CCK_1) is encrypted using the UEV which is created using a burned-in part (Fig. 26, #118) and a provider part (Fig. 26, #121). Therefore, Richard's second key (PK and SK) is used to decrypt the content (Fig. 26, `[CONTENT]SK + SK -->> CONTENT`) and as such, Richards discloses "***determining a second key for decrypting content on a broadcast channel***". Further, Richards then discloses

"***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel***" because Richards discloses the second key (SK and PK) where when PK is used, SK is known to the participant (set-top-box) (Fig. 26, #152) and SK is received over a broadcast channel (Fig. 26, #152).

7. Applicant's response (p. 11) further argues that both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant". However, as clearly seen in Fig. 26, to decrypt SK, the set-top-box must know PK (Fig. 26, #152). Therefore, because when the encrypted SK is received ([SK]PK), the unit already knows PK, Richards is maintained to anticipate this limitation.

8. Applicant's response (p. 12) reiterates the above arguments, arguing that Richards lacks "***receiving a second key for decrypting content on a broadcast channel; decrypting the second key with the first key***". However, Richards discloses a second key (PK and SK) for decrypting content on a broadcast channel (Fig. 26, #159) and decrypting the second key with the first key (CCK_1) (Fig. 26, ##138, 144, 152).

9. Applicant's response (p. 13) argues that Richards lacks "***receiving a second key for decrypting content on a broadcast channel encrypted with the first key***". However, as described above, Richards discloses receiving a second key/SK and PK for decrypting content on a broadcast channel (Fig. 26, #159) encrypted with a first key/CCK_1 (Fig. 26).

10. Applicant's response (pp. 13-18) argues that Richards lacks "**receiving a second key for decrypting content on a broadcast channel encrypted with the first key, receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a**

first part known to the participant in the transmission and a second part sent on the broadcast channel." However, as described above, Richards discloses receiving a second key (SK and PK) for decrypting content on a broadcast channel (Fig. 26, #159) encrypted with a first key/CCK_1 (Fig. 26, #138), receiving an updated first key/CCK_1 after a first time period has elapsed (Fig. 22), and receiving an updated second key (SK and PK) after a second time period has elapsed (Fig. 26), wherein the second key (SK and PK) is updated in two parts (SK and PK), a first part known to the participant in the transmission (PK) and a second part sent on the broadcast channel (SK) (Fig. 26).

11. Applicant's response (pp. 18-19) relies on the previous arguments. However, as described above, those arguments are not persuasive.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1-5, 10-11, 13-16 & 18-24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,690,795 to **Richards**.

Regarding claims 1-5, 11, 13-14 & 22-24, Richards discloses determining a registration key/UEV specific to a participant/set top box in a transmission (Fig. 26, #130 & col. 20, lines 61-67), determining a first key/CCK_1 (Fig. 26, #133), encrypting the first key/CCK_1 with the

registration key (Fig. 26, #133), sending the encrypted first key/[CCK_1]UEV to the participant in the transmission/set top box (Fig. 26, #133), determining a second key/PK and SK for decrypting content on a broadcast channel (Fig. 26, #159), encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key/CCK after a first time period has elapsed (Fig. 23) and updating the second key/SK and PK after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part/PK known to the participant in the transmission and a second part/SK send on the broadcast channel (Fig. 26).

Regarding claim 10, Richards discloses transmitting the encrypted first key/PK and transmitting the encrypted second key/SK (col. 9, line 58 – col. 10, line 5).

Regarding claims 15 & 16, Richards discloses in a wireless system (col. 20, lines 61-67) determining a registration key/UEV specific to a participant/set top box in a transmission (Fig. 26, #130), determining a first key/CCK_1 (Fig. 26, #133), encrypting the first key/CCK_1 with the registration key (Fig. 26, #133), sending the encrypted first key/[CCK_1]UEV to the participant in the transmission/set top box (Fig. 26, #133), determining a second key/PK and SK, encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key/CCK after a first time period has elapsed (Fig. 23) and updating the second key/SK and PK after a second time period has elapsed, wherein the second key is updated in two parts (SK and PK), the first part/PK known to the participant in the transaction and a second part/SK send on a broadcast channel (Fig. 26), a user identification unit/set-top box (col. 4, lines 55-62), operative to recover a short-time key/SK for decrypting a broadcast message/content (col. 9, lines 11-33), comprising a processing unit/decryption hardware to decrypt key information (col. 9, lines 11-33) and a

mobile equipment unit/decryption hardware adapted to apply the short-time key for decrypting the broadcast message/content (col. 4, lines 55-62 & col. 9, lines 11-33).

Regarding claim 18, Richards discloses the memory storage unit storing a broadcast access key/PK and wherein the processing unit decrypts the short-time key/SK using the broadcast access key/PK (col. 5, lines 45-64 & col. 9, lines 56-63).

Regarding claim 19, Richards discloses the short-time key/SK being updated at a first frequency (col. 9, lines 32-36 & Fig. 16).

Regarding claim 20, Richards discloses the broadcast access key/PK being updated at a second frequency less than the first frequency (Figs. 9 & 10).

Regarding claim 21, Richards discloses a video service (col. 2, lines 39-55).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 4 above, in further view of "FOLDOC, Free On-Line Dictionary Of Computing" by **LinuxGuruz**. Richards discloses using the system for distributing information on computer networks, but lacks specifically Internet Protocol packets. However, LinuxGuruz teaches that Internet Protocol packets are widely used on Ethernet networks for packet routing (§Internet Protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to broadcast Internet Protocol packets. One of ordinary skill in the art would have been motivated to perform such a modification because Internet Protocol packets are used on Ethernet networks, as taught by LinuxGuruz (§Internet Protocol).

16. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claim 3 above, in further view of Applied Cryptography, Second Edition by **Schneier**.

Regarding claim 7, Richards lacks calculating a registration key information message and transmitting the registration key information message. However, Schneier teaches that no encryption key should be used for an indefinite period (p. 183, §8.10) and should be replaced (p. 184, ¶3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to update the registration key and hence calculate a registration key information message and transmit the registration key information message. One of ordinary skill in the art would have been motivated to perform such a modification to update the registration key, as taught by Schneier (pp. 183-184).

Regarding claim 8, Richards discloses calculating a first key/PK information message/new encrypted key and transmitting the first key information message (col. 10, lines 1-5).

Regarding claim 9, Richards discloses calculating a second key/PK information message/new encrypted key and transmitting the second key information message (col. 9, lines 58-62).

17. Claims 12 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Richards**, as applied to claims 11 & 15 above, in further view of U.S. Patent 6,073,122 to **Wool**. Richards discloses storing the second key/SK in a memory storage unit (col. 5, lines 60-63), but lacks the first key stored in secure memory storage unit. However, Wool teaches that set-top boxes often contain secure memory to minimize piracy of encryption keys stored (col. 1, lines 44-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the first key in a secure memory storage unit. One of ordinary skill in the art would have been motivated to perform such a modification to minimize piracy of encryption keys stored, as taught by Wool (col. 1, lines 44-52).

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

July 26, 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100